J. Symbolic Computation (1988) **6**, 149–167

Gröbner Bases and Primary Decomposition of Polynomial Ideals

PATRIZIA GIANNI, BARRY TRAGER* AND GAIL ZACHARIAS†

IBM Research and University of Pisa, Pisa, Italy
**IBM Research, P.O. Box 218, Yorktown Heights, NY 10598, USA*
†*MIT AI Laboratory, 545 Technology Square, Cambridge, MA 02139, USA*

We present an algorithm to compute the primary decomposition of any ideal in a polynomial ring over a factorially closed algorithmic principal ideal domain R. This means that the ring R is a constructive PID and that we are given an algorithm to factor polynomials over fields which are finitely generated over R or residue fields of R. We show how basic ideal theoretic operations can be performed using Gröbner bases and we exploit these constructions to inductively reduce the problem to zero dimensional ideals. Here we again exploit the structure of Gröbner bases to directly compute the primary decomposition using polynomial factorization. We also show how the reduction process can be applied to computing radicals and testing ideals for primality.

1. Introduction

A fundamental construction in commutative algebra is the primary decomposition of ideals. From an algebraic point of view this generalizes the operation of factorization into products of irreducible elements, while it is connected from a geometric viewpoint with the decomposition of a variety into its irreducible components. In this paper we present an algorithm to compute the primary decomposition of any ideal in a polynomial ring over a factorially closed algorithmic principal ideal domain (Ayoub, 1982). The rational integers $\mathbf{Z}$ form such a ring, but more generally this means that the ring R is a constructive PID and that we are given an algorithm to factor polynomials over fields which are finitely generated over R or residue fields of R. In particular this is true if R is any prime ring (Seidenberg, 1974; Davenport & Trager, 1981).

Algorithms for primary decomposition in polynomial rings over $\mathbf{Z}$ have been presented by Seidenberg (1978) and Ayoub (1982). Seidenberg was able to present a simplified construction when the base ring was a field by reducing the problem to zero-dimensional ideals (Seidenberg, 1978, Theorem 9). In the more general case when the base ring was the integers, he was forced to give a more indirect construction involving first computing all the associated primes, and then isolating the primary component associated with each prime. Ayoub attempted to generalize his construction for fields to principal ideal domains. She presented an algorithm which proceeded by induction on the number of variables in the polynomial ring, rather than on the dimension of auxiliary ideals at each stage of the process. Subsequently Seidenberg (1984) investigated more general rings R and presented conditions on R which are sufficient to allow the computation of primary decompositions in polynomial rings over R.

We base our construction on the Gröbner basis algorithm, a very powerful tool in computational ring theory (Buchberger, 1983). This method was introduced in 1965 by

0747-7171/88/020149+19 $03.00/0

Buchberger to solve systems of polynomial equations (Buchberger, 1965). It provides a canonical (relative to a monomial ordering) set of generators for an ideal which facilitates testing ideal membership and contraction of ideals of subrings. Lazard (1985) has also exploited the structure of a Gröbner basis to give a very efficient primary decomposition algorithm for the special case of polynomial rings in two variables over fields.

Our construction of the primary decomposition is based on an induction on dimension which generalizes the one presented by Seidenberg for the field case. We use localization at principal primes in place of quotient field formation to decrease the dimension and we present in Proposition 3.7 the fundamental construction which enables us to reduce the primary decomposition computation to its zero-dimensional counterpart. We show how the zero-dimensional problem can be solved by exploiting the structure of Gröbner bases.

In the first section we introduce our notations and recall the known properties of Gröbner bases which we will use. The next section shows how basic ideal-theoretic operations such as contractions, intersections, and ideal quotients can be directly computed using Gröbner bases. Next we present the properties of Gröbner bases for zero-dimensional ideals. This is used to develop primary decomposition algorithms, first for general zero-dimensional ideals over PID's, and later a simpler and more efficient one when the coefficient ring is a field and the ideal is in general position. Finally we develop our fundamental construction which enables us to reduce the decomposition of general ideals to the zero-dimensional case. We also show how the reduction process can be applied to other problems, specifically computing radicals and testing ideals for primality.

2. Definitions

Let R be a Noetherian commutative ring with identity.
We use the following standard notation:

If S is a multiplicatively closed subset of R, then $S^{-1}R = \{r/s \mid s \in S\}$ denotes the ring of fractions of R with respect to S..
If $f \in R$ then $R_f = S^{-1}R$, where $S = \{f^n\}$, is the localization of R at f.
If $P \subset R$ is a prime ideal then $RP = S^{-1}R$, where $S = R - P$, is the localisation of R at P.
If I, J are ideals in R then $I{:}J = \{a \mid aJ \subset I\}$ is the ideal quotient of I and J.
If $I \subset R$ is an ideal then $\sqrt{I} = \{a \mid a^m \in I \text{ for some } m\}$ is the radical of I.

We will say that an ideal I is "given" if we are given a finite set of generators for I.

DEFINITION 2.1. We say that linear equations are solvable in R if:

(a) (ideal membership) Given $a, a_1, \ldots, a_m \in R$ it is possible to decide whether a is in the ideal $(a_1, \ldots, a_m)R$ and if so, find $b_1, \ldots, b_m$ such that $a = \Sigma b_i a_i$.
(b) (syzygies) Given $a_1, \ldots, a_m \in R$ one can find a finite set of generators for the R-module $\{(b_1, \ldots, b_m) \in R^m \mid \Sigma b_i a_i = 0\}$.

In all that follows we assume that R is a ring in which linear equations are solvable. We now review the definitions and basic properties of Gröbner bases and associated concepts.

DEFINITION 2.2. A total order $>$ on N^n is compatible with the semi-group structure if

(i) $A \geqslant 0$ for all $A \in N^n$.
(ii) $A > B \Rightarrow A + C > B + C$ for all $A, B, C \in N^n$.

We now fix a compatible order $>$. Note that such an order is necessarily a well-ordering (Zacharias, 1978).

DEFINITION 2.3. For any non-zero $f \in R[x] = R[x_1, \ldots, x_n]$, write

$$f = cx^A + f'$$

with $c \in R$, $c \neq 0$, and $A > A'$ for every non-zero term $c'x^{A'}$ of f'. With this notation we set

$$\mathrm{lt}(f) = cx^A, \text{ the leading term of } f.$$

$$\mathrm{lc}(f) = c, \text{ the leading coefficient of } f.$$

$$\deg(f) = A, \text{ the degree of } f.$$

For a subset G of $R[x]$, we define

$$\mathrm{Lt}(G) = \text{the ideal generated by } \{\mathrm{lt}(g) \mid g \in G\}, \text{ the leading term ideal of } G.$$

By convention we let $\mathrm{lt}(0) = \mathrm{lc}(0) = 0$ and $\deg(0) = -\infty$.

DEFINITION 2.4. $f \in R[x]$ is reducible modulo $G \subset R[x]$ if f is non-zero and $\mathrm{lt}(f) \in \mathrm{Lt}(G)$. Otherwise f is reduced modulo G.

PROPOSITION 2.5. (Reduction algorithm) *Given f and $G = \{g_1, \ldots, g_m\}$ in $R[x]$, it is possible to construct f' such that $f = f' \bmod (g_1, \ldots, g_m)R[x]$ and f' is reduced modulo G.*

PROOF. The ideal membership condition on R insures that we can decide whether f is reducible modulo G, and if so, find terms t_i such that $\mathrm{lt}(f) = \Sigma t_i \, \mathrm{lt}(g_i)$. If f is not reducible, then $f' = f$ will do. Otherwise let $f_1 = f - \Sigma t_i g_i$. By construction, the leading term of $\Sigma t_i g_i$ cancels the leading term of f, so $\deg(f_1) < \deg(f)$. Thus by induction on the well-ordering $<$ we can find a reduced f' with $f' \equiv f_1 \bmod (g_1, \ldots, g_m)$. But $f \equiv f_1$ so $f \equiv f'$ as required. □

REMARK. It is clear from the proof that the non-constructive version of Proposition 2.5 also holds: For any f and G (whether explicitly given or not), there exists a reduced f' with $f \equiv f'$ modulo the ideal generated by G.

DEFINITION 2.6. A subset G of an ideal $I \subset R[x]$ is a Gröbner basis for I if $\mathrm{Lt}(G) = \mathrm{Lt}(I)$, that is if every non-zero element of I is reducible modulo G. G is a minimal Gröbner basis if additionally every $g \in G$ is non-zero and reduced modulo $G - \{g\}$.

If g is reducible modulo $G - \{g\}$, i.e. $\mathrm{lt}(g) \in \mathrm{Lt}(G \neq \{g\})$, then $\mathrm{Lt}(G - \{g\}) = \mathrm{Lt}(G)$. Thus $G - \{g\}$ is a Gröbner basis for I if G is. In particular any given Gröbner basis can be made minimal by simply removing those elements which are reducible modulo the others.

The following proposition describes the fundamental property of Gröbner bases.

PROPOSITION 2.7. *Let G be a Gröbner basis for $I \subset R[x]$. Then $f \in I$ if and only if applying the reduction algorithm* (Proposition 2.5) *to f returns* 0.

PROOF. Let f be a non-zero element of $R[x]$ and let f' be as in Proposition 2.5. Since $G \subset I$, $f \equiv f' \bmod I$. Thus if $f' = 0$ then $f \in I$ and we are done. Conversely, if $f \in I$ then $f' \in I$ and hence $\mathrm{lt}(f') \in \mathrm{Lt}(I) = \mathrm{Lt}(G)$. But f' is reduced modulo G, so we must have $f' = 0$. □

COROLLARY 2.8. If G *is a given Gröbner basis for* I *then ideal membership in* I *is decidable.*

COROLLARY 2.9. *If* G *is a Gröbner basis for* I *then* G *generates* I.

We also record the following useful consequence of previous results:

COROLLARY 2.10. *If* $J \subset I$ *are ideals in* $R[x]$ *and* $\mathrm{Lt}(I) = \mathrm{Lt}(J)$ *then* $I = J$.

PROOF. J forms a (non-finite) Gröbner basis for I, so by the remark following Proposition 2.5, we may conclude that J generates I. But since J is an ideal, it only generates itself, so $J = I$. □

The importance of Gröbner bases in constructive algebra derives from the following fact:

PROPOSITION 2.11. *One can compute a Gröbner basis for an ideal in* $R[x]$ *from any given set of generators.*

PROOF. See Trinks (1978) or Zacharias (1978). □

We remark that the Gröbner basis algorithm automatically produces a basis for the syzygy module of the generators. Thus it can be used to demonstrate that $R[x]$ satisfies both the computability conditions of Definition 2.1 whenever R does.

The computation of Gröbner bases takes a particularly simple form when the coefficient ring R is a Principal Ideal Domain (PID) or a field. In fact the algorithm was originally discovered in the context of fields (Buchberger, 1965; 1970; 1976). See also (Buchberger, 1979) for some additional results which can be used to improve the efficiency of the algorithm.

Finally, we note that our definition of Gröbner bases is the least restrictive one possible, in the sense that there exist definitions in the literature which place additional conditions on the leading coefficients and/or non-leading terms of the basis elements. All the algorithms presented in this paper can of course be applied to any such stricter types of Gröbner bases, provided only that the condition of Definition 2.6 is satisfied.

3. Operations on Ideals

In this section we discuss the use of Gröbner bases to perform some basic ideal operations in $R[x]$. Most of the constructions we describe are based on an observation by D. Spear (1977) that Gröbner bases computed with respect to the lexicographical order on monomials have the effect of eliminating the more "main" variables. The following proposition describes this property in more detail.

PROPOSITION 3.1. *Let* I *be an ideal in* $R[y, x] = R[y_1, \ldots, y_n, x_1, \ldots, x_m]$. *Given any two orders* $>_1$ *and* $>_2$ *on monomials in* x *and* y *respectively, define an order* $>$ *by* $x^A y^B > x^{A'} y^{B'}$ *if* $x^A >_1 x^{A'}$, *or if* $x^A = x^{A'}$ *and* $y^B >_2 y^{B'}$. *If* $G \subset R[y, x]$ *is a Gröbner basis for* I *with respect to* $>$ *then*

(*i*) G *is a Gröbner basis for* I *with respect to the order* $>_1$ *on* $(R[y])[x]$, *the polynomial ring in* $x_1, \ldots, x_m$ *with coefficients in* $R[y]$.

(*ii*) $G \cap R[y]$ *is a Gröbner basis for* $I \cap R[y]$ *with respect to the order* $>_2$.

PROOF. (i) By the definition of $>$, we have $\mathrm{lt}_{>}(\mathrm{lt}_{>_1}(f)) = \mathrm{lt}_{>}(f)$ for any $f \in R[y, x]$. Hence

$$\mathrm{Lt}_{>}(\mathrm{Lt}_{>_1}(G)) = \mathrm{Lt}_{>}(G) = \mathrm{Lt}_{>}(I) = \mathrm{Lt}_{>}(\mathrm{Lt}_{>_1}(I))$$

Thus by Corollary 2.10, $\mathrm{Lt}_{>_1}(G) = \mathrm{Lt}_{>_1}(I)$.

(ii) Since no term involving any x_i can be $>$-larger than a term involving only the y_j, a polynomial whose leading term is in $R[y]$ cannot involve any x_i in the remaining, smaller, terms. In other words, $\mathrm{lt}_{>}(g) \in R[y] \Leftrightarrow g \in R[y]$. Hence

$$\mathrm{Lt}_{>}(G \cap R[y]) = \mathrm{Lt}_{>}(G) \cap R[y] = \mathrm{Lt}_{>}(I) \cap R[y] = \mathrm{Lt}_{>}(I \cap R[y])$$

So $G \cap R[y]$ is a Gröbner basis for $I \cap R[y]$ with respect to $>$. But $>$ coincides with $>_2$ on $R[y]$. □

Part (i) of the proposition shows that in order to compute Gröbner basis with coefficients in a ring $R[y]$ which is itself a polynomial ring over a base ring R, we can instead group the coefficient variables y and ring variables x together using an appropriate order $>$ (extending the desired order $>_1$) and apply the algorithm over R itself. This is of great practical importance when the base ring R is a field or a PID, for in those cases the Gröbner basis computation over R is much simpler than the general algorithm which would have to be used if we were to work directly over the coefficient ring $R[y]$.

In the remainder of this paper, we will often appear to require the calculation of Gröbner bases with coefficients in polynomial rings constructed from an initial base ring. It is a consequence of this proposition that in practice all our constructions can be performed using the simpler PID (respectively field) variant of the Gröbner basis algorithm, provided the original base ring is a PID (respectively a field).

Part (ii) of the proposition shows that we can compute the contraction of an ideal to a coordinate subring: We simply compute the Gröbner basis for the ideal, with respect to an order $>$ based on whatever order $>_2$ we want for the contraction. Then the elements of the Gröbner basis which involve only the subring variables give a Gröbner basis for the contraction.

EXAMPLE. Consider the ideal $I = (xy + y, xz + 1) \subset Q[z, y, x]$. Using the full lexicographical order with $x > y > z$, we can compute a minimal Gröbner basis $G = \{yx + y, zx + 1, yz - y\}$ for I. Since $G \cap Q[z, y] = \{yz - y\}$, Proposition 3.1(ii) implies that $I \cap Q[z, y] = (yz - y)Q[z, y]$. Proposition 3.1(i) states that G is also a Gröbner basis for I when it is considered as an ideal in the polynomial ring $Q[z, y][x]$ with variable x and coefficients in $Q[z, y]$. In other words, $\mathrm{Lt}_x(I) = \mathrm{Lt}_x(G)$ where Lt_x refers to leading terms taken with respect to the ordering of powers of x only. Note that in the interpretation, G is not a minimal Gröbner basis, for we have

$$\mathrm{lt}_x(xy + y) = xy = y(xz) - x(yz - y) = y\,\mathrm{lt}_x(xz + 1) - x\,\mathrm{lt}_x(yz - y)$$
$$\in (\mathrm{lt}_x(xz + 1), \mathrm{lt}_x(yz - y)).$$

Thus a minimal Gröbner basis for $I \subset (Q[z, y])[x]$ is $G' = \{xz + 1, yz - y\}$. Note that G' is not a Gröbner basis for I when all the variables are considered, because then $\mathrm{lt}(yz - y) = yz$ and $xy \notin (xz, yz)$. As this example shows, the price for computing the Gröbner bases over Q when we are only interested in the basis over $Q[z, y]$ is the construction of some unnecessary basis elements. The advantage is the ability to use simpler versions of the algorithms.

A number of useful ideal operations which can be expressed in terms of coordinate subring contractions are listed below.

COROLLARY 3.2. *Let I and J be given ideals in $R[x]$. Then the following can be computed*:

(i) $I \cap J$.
(ii) $I: J$, *if the generators of J aren't zero divisors.*
(iii) *The kernel of a given homomorphism* $\varphi: R[y] \mapsto R[x]/I$.
(iv) *The ideal of polynomial relations among* $f_1, \ldots, f_m \in R[x]$.
(v) $IR[x]_f \cap R[x]$ *for any nonzero divisor* $f \in R[x]$.

PROOF. (i) Let t be a new indeterminate and observe that

$$I \cap J = (tI, (t-1)J)R[x, t] \cap R[x].$$

We note that we could compute the intersection directly by constructing the basis for an appropriate syzygy module, but the approach through subring contraction is simpler and more efficient. This is because the contraction computes the basis for the intersection of the ideals directly, without needing to first construct and store the explicit expression of each element as a linear combination of generators of both I and J.

(ii) Let $J = (f_1, \ldots, f_m)$. Then $I: J = \bigcap_i I: (f_i)$, so $I: J$ can be constructed provided each $I: (f_i)$ can. Now $I \cap (f_i)$ can be computed by (i), and if $\{g_1, \ldots, g_k\}$ is a basis for $I \cap (f_i)$ then $\{g_1/f_i, \ldots, g_k/f_i\}$ is a basis for $I: (f_i)$.
(iii) If the homomorphism φ is given by $\varphi(y_i) = f_i$, with $f_i \in R[x]$, the kernel is the ideal $((y_i - f_i), I)R[x, y] \cap R[y]$
(iv) Take $I = 0$ in (iii).
(v) $R[x]_f \simeq R[x, t]/(tf - 1)$, where t is a new indeterminate. Thus

$$IR[x]_f \cap R[x] = (I, tf - 1)R[x, t] \cap R[x]. \quad \square$$

For example consider the ideal $I = (12, xy + 2) \subset \mathbf{Z}[y, z]$. In order to compute $I \cap (y)$ we first find the Gröbner basis for

$$(It, (t-1)y) = (12t, xyt + 2t, ty - y) \subset \mathbf{Z}[y, x, t]$$

using an order which puts t first. For example with total lexicographical order with $t > x > y$, the Gröbner basis is

$$G = (yxt - xy, yt - y, 2t + yx, 12y, xy^2 + 2y, 6xy).$$

Contracting this to $\mathbf{Z}[y, x]$ we find that

$$I \cap (y) = (12y, xy^2 + 2y, 6xy).$$

Dividing by y we see that $(I: y) = (6x, 12, xy + 2)$. In order to divide out all powers of y from I, we compute

$$I\mathbf{Z}[y, x]_y \cap \mathbf{Z}[y, x].$$

Proceeding as in part (v) above, we consider the ideal $(I, ty - 1) \subset \mathbf{Z}[y, x, t]$.

$$G = (ty - 1, 2t + x, 3x^2, 6x, 12, xy + 2)$$

is a Gröbner basis for it in lexicographical order, so by contracting the basis we find that

$$I\mathbf{Z}[y, x]_y \cap \mathbf{Z}[y, x] = (3x^2, 6x, 12, xy + 2).$$

Proposition 3.1(ii) shows in particular that if G is a Gröbner basis for $I \subset R[x]$ then $G \cap R$ generates $I \cap R$. We can in fact characterize the situation fully as follows:

PROPOSITION 3.3. *Let I be an ideal in $R[x]$ and let π: $R[x] \mapsto (R/I \cap R)[x]$ be the quotient map. Then for $G \subset I$ we have*

(*i*) *If G is a Gröbner basis for I then $G \cap R$ generates $I \cap R$ and $\pi(G)$ is a Gröbner basis for $\pi(I)$.*

(*ii*) *G is a minimal Gröbner basis for I if and only if $G \cap R$ is a minimal basis for $I \cap R$, $\pi(G - G \cap R)$ is a minimal Gröbner basis for $\pi(I)$, and $\pi(\mathrm{lt}(g)) \neq 0$ for all $g \in G - G \cap R$.*

PROOF. Since $\pi(\mathrm{lt}(f))$ is either 0 or $\mathrm{lt}(\pi(f))$, we have $\pi(\mathrm{Lt}(I)) \subset \mathrm{Lt}(\pi(I))$, and, conversely, given $f \in I$, we can write $f = f_0 + f_1$ where $\pi(f_0) = 0$ and $\pi(\mathrm{lc}(f_1)) \neq 0$. In particular, $f_0 \in I$ and so $f_1 \in I$ and $\mathrm{lt}(\pi(f)) = \mathrm{lt}(\pi(f_1)) = \pi(\mathrm{lt}(f_1)) \in \pi(\mathrm{Lt}(I))$. Thus we observe that $\pi(\mathrm{Lt}(I)) = \mathrm{Lt}(\pi(I))$. The result now follows from the definitions and Proposition 3.1(ii). □

Finally, we consider the construction of the ring of fractions of $R[x]$ with respect to multiplicative subsets of R. We first observe that Gröbner bases are well behaved under this operation.

PROPOSITION 3.4. *Let S be a multiplicatively closed subset of R. If G is a Gröbner basis for an ideal $I \subset R[x]$ then it is a Gröbner basis for $S^{-1}I \subset (S^{-1}R)[x]$.*

PROOF. We have $\mathrm{Lt}(S^{-1}I) = S^{-1}\mathrm{Lt}(I) = S^{-1}\mathrm{Lt}(G)$, i.e. the leading terms of elements of G generate $\mathrm{Lt}(S^{-1}I)$ in $S^{-1}R[x]$. □

Thus computing with Gröbner bases in $(S^{-1}R)[x]$ presents no special problems. An important construction which we need to consider now is the saturation $S^{-1}I \cap R[x]$ with respect to S of an ideal $I \subset R[x]$. We note that this operation can be determined from the behaviour of the leading term ideal, in the following sense:

LEMMA 3.5. *Let $T \subset S$ be multiplicatively closed subsets of R, and let I be an ideal in $R[x]$ if*

$$S^{-1}\mathrm{Lt}(I) \cap R[x] = T^{-1}\mathrm{Lt}(I) \cap R[x]$$

then

$$S^{-1}I \cap R[x] = T^{-1}I \cap R[x].$$

PROOF. We have

$$\begin{aligned}
\mathrm{Lt}(S^{-1}I \cap T^{-1}R[x]) &\subseteq \mathrm{Lt}(S^{-1}I) \cap T^{-1}R[x] \\
&= S^{-1}\mathrm{Lt}(I) \cap T^{-1}R[x] \\
&= T^{-1}(S^{-1}\mathrm{Lt}(I) \cap R[x]) \quad \text{because } T \subset S \\
&= T^{-1}(T^{-1}\mathrm{Lt}(I) \cap R[x]) \quad \text{by assumption} \\
&= T^{-1}\mathrm{Lt}(I) \\
&= \mathrm{Lt}(T^{-1}I)
\end{aligned}$$

Since $S^{-1}I \cap T^{-1}R[x] \supset T^{-1}I$, we obtain $\mathrm{Lt}(S^{-1}I \cap T^{-1}R[x]) = \mathrm{Lt}(T^{-1}I)$. Thus by Corollary 2.10 we have

$$S^{-1}I \cap T^{-1}R[x] = T^{-1}I.$$

Taking the intersection with $R[x]$ completes the proof. □

We remark that taking $T = \{1\}$ shows that I is saturated with respect to S if $\mathrm{Lt}(I)$ is. More generally, the lemma states that we may attempt to compute the saturation with respect to S using a smaller multiplicative set T, provided the change does not affect the behaviour of the leading term ideal.

PROPOSITION 3.6. *Let S be a multiplicatively closed subset of R, I an ideal in $R[x]$. If for some $s \in S$,*

$$S^{-1}\mathrm{Lt}(I) \cap R[x] = (\mathrm{Lt}(I)R_s[x]) \cap R[x] \qquad (*)$$

then

$$S^{-1}I \cap R[x] = IR_s[x] \cap R[x].$$

PROOF. Apply the lemma with $T = \{s^n\}$. □

Since we know how to compute $IR_s[x] \cap R[x]$ by Corollary 3.2(v), $S^{-1}I \cap R[x]$ can be computed if we can find an $s \in S$ satisfying condition (*). Thus Propostion 3.6 reduces the problem of computing the saturation $S^{-1}I \cap R[x]$ of an arbitrary ideal I in $R[x]$ to an analogous problem for ideals generated by terms. This is equivalent to solving the problem for finite sets of ideals in R, and whether it can be done depends of course on the given R and S.

Of particular interest to us is the localization R_P at a prime ideal $P \subset R$, i.e. the case where $S = R - P$. While we do not know of any general algorithms to compute the saturations of ideals in R with respect to arbitrary prime ideals P, the problem can be solved in the case where P is a principal ideal. The following proposition will be central to a dimension reduction process which will be developed later in the paper.

PROPOSITION 3.7. *Let R be an integral domain, $(p) \subset R$ a principal prime ideal. For any given ideal $I \subset R[x]$ it is possible to find $s \in R - (p)$ such that*

$$IR_{(p)}[x] \cap R[x] = IR_s[x] \cap R[x].$$

In particular $IR_{(p)}[x] \cap R[x]$ can be computed

PROOF. Since R is a domain, $\cap (p^k) = 0$. Thus for any non-zero element r of R there exists a k such that $r \in (p^k)$, and $r \notin (p^{k+1})$. Thus $r = sp^k$ for some $s \notin (p)$. We can compute k and s by applying the ideal membership algorithm. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I. Express $\mathrm{lt}(g_i)$ as $\mathrm{lt}(g_i) = s_i p^{k_i} x^{A_i}$, where $s_i \notin (p)$ as described above. Then $\mathrm{Lt}(I) = (s_i p^{k_i} x^{A_i})$ while $\mathrm{Lt}(I)R_{(p)}[x] \cap R[x] = (p^{k_i} x^{A_i})$. Thus in order to apply Proposition 3.6, we only need to find an s such that every s_i is invertible in $R_s[x]$. The choice $s = \prod s_i$ satisfies this condition. (In fact any common multiple of the radicals of s_i will be sufficient. Furthermore it is only necessary to consider those i with $(p^{k_i} x^{A_i})$ minimal.) □

Finally we note a very useful special case of Proposition 3.7.

COROLLARY 3.8. *Let R be an integral domain, K the quotient field of R. Then for any given ideal $I \subset R[x]$ it is possible to compute $IK[x] \cap R[x]$.*

PROOF. Apply the proposition with $p = 0$. □

REMARK. When $p = 0$, the s of Proposition 3.7 is simply the product of the leading coefficients of a Gröbner basis for I.

4. Primality Test

As an application of the results developed in the previous section, we now present an algorithm for testing the primality of ideals in $R[x]$. We first recall the following basic facts:

LEMMA 4.1. *An ideal $I \subset R[x]$ is prime if and only if $I \cap R$ is prime and the image of I in $(R/I \cap R)[x]$ is prime.*

PROOF. Zariski & Samuel (1975) Chapter III, Theorem 11. □

LEMMA 4.2. *Let R be an integral domain, K the quotient field of R. If I is an ideal of $R[x]$ such that $I \cap R = (0)$ then I is prime if and only if $IK[x]$ is prime and $I = IK[x] \cap R[x]$.*

PROOF. Zariski & Samuel (1975) Chapter IV, Corollary 1 to Theorem 16. □

We assume that we have a primality test for ideals in R and that we can test the irreducibility of univariate polynomials over quotient fields of residue rings of $R[x]$ (this will be the case for instance if R is a prime field or Z). Then we obtain:

PROPOSITION 4.3. *It is possible to decide the primality of ideals in $R[x]$*

PROOF. Proceeding by induction on the number of variables we may assume that we have an ideal I in $R[x_1]$. We can compute $I^c = I \cap R$ by Proposition 3.1(ii). If I^c is not prime then neither is I and we are done. Otherwise by Lemma 4.1, we need only to test the primality of the image of I in $R/I^c[x_1]$. Replacing R by R/I^c, we may assume R is an integral domain and $I \cap R = (0)$. Let K be the quotient field of R. Then $IK[x_1]$ is a principal ideal and hence we can test its primality by checking the irreducibility of its generator. We can compute $IK[x_1] \cap R[x_1]$ by Corollary 3.8. Thus we can test the primality of I by Lemma 4.2. □

ALGORITHM PT $(R; x; I)$. Primality test

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$.
Assumptions: (none)
Output: TRUE if I is prime, otherwise FALSE.
Step 1: If $n = 0$ then if $I \subset R$ is prime the return TRUE otherwise return FALSE.
Step 2: Compute $J = I \cap R[x_2, \ldots, x_n]$. [Proposition 3.1(ii)]
Step 3: If PT $(R; x_2, \ldots, x_n; J) =$ FALSE then return to FALSE.
Step 4: Let $R' = R[x_2, \ldots, x_n]/J$, $I' = IR'[x_1]$, $K' =$ the quotient field of R'.

Step 5: Compute $I'K'[x_1] = (f)$.
Step 6: If f is not irreducible over K' then return FALSE.
Step 7: Compute $I^{ec} = I'K'[x_1] \cap R'[x_1]$. [Corollary 3.8]
Step 8: If $I^{ec} \subset I'$ then return TRUE, otherwise return FALSE.

5. Zero-dimensional Ideals

We now begin a deeper study of the properties of Gröbner bases by examining the structure of zero-dimensional ideals. First we show that under certain conditions we can determine whether an ideal is zero-dimensional by simply inspecting its Gröbner basis.

LEMMA 5.1 *Let $I \subset R[x]$ be an ideal such that $I \cap R$ is zero-dimensional. Then I is zero-dimensional if and only if $R[x]/I$ is integral over R.*

PROOF. $\Leftarrow$: If $R[x]/I$ is integral over R then it is also integral over the subring $R/I \cap R \subset R[x]/I$. Thus $R/I \cap R$ and $R[x]/I$ have the same dimension.

$\Rightarrow$: Let $I = \cap Q_k$ be a primary decomposition of I, and let $M_k = \sqrt{Q_k}$. By assumption, M_k is maximal. Since $M_k \cap R$ contains $I \cap R$, it is zero-dimensional and hence maximal. Therefore, by the Nullstellensatz, the field $R[x]/M_k$ is a finite algebraic extension of the subfield $R/M_k \cap R$. In particular, for each i, M_k contains a monic polynomial $f_{i,k}(x_i)$. Then $f_{i,k}(x_i)^N \in Q_k$ for some N, and so $\prod_k f_{i,k}(x_i)^N \in I$ is an equation of integral dependence for $x_i \bmod I$. □

The requirement that $I \cap R$ be zero-dimensional cannot be omitted. For instance consider $R = Z_{(2)}$, the localization of Z at the prime ideal generated by $2 \in Z$. Then the ideal $I = (2x - 1)R$ in $R[x]$ is maximal but contains no monic polynomials, so $x \bmod I$ is not integral over R. And indeed $I \cap R = (0)$ is not zero-dimensional.

We note however that the condition that $I \cap R$ be zero-dimensional for every zero-dimensional ideal $I \subset R[x]$ is satisfied in Hilbert rings (see Kaplansky, 1968). In particular the condition holds for polynomial rings with coefficients in a field. Furthermore, it follows from the lemma that if I and $I \cap R[x]$ are zero-dimensional then so is $I \cap R[x_i, \ldots, x_n]$ for any i.

The following proposition gives an effective criterion for detecting integral extensions.

PROPOSITION 5.2. *$R[x]/I$ is integral over R if and only if $(x_1, \ldots, x_n) \subset \sqrt{\mathrm{Lt}(I)}$.*

PROOF. $\Rightarrow$: Each $x_i + I \in R[x]/I$ is integral over R, so for each i, I contains a monic polynomial $f(x_i) \in R[x_i]$. Then $\mathrm{lt}(f(x_i)) \in \mathrm{Lt}(I)$, but the leading term of $f(x_i)$ is just a power of x_i.

$\Leftarrow$: We will show that $R[x]/I$ in finitely generated as an R-module, which implies that it is integral over R. Suppose $x_i^{m_i} \in \mathrm{Lt}(I)$, and consider the finitely generated R-module

$$K = \sum_{a_i < m_i} R x_1^{a_1} \ldots x_n^{a_n}.$$

We claim that the R-module map $\pi: K \mapsto R[x]/I$, defined by $\pi(h) = h + I$, is surjective. Let f be an element of $R[x]$ and consider $f + I \in R[x]/I$. We may assume $f \notin I$, since $0 + I$ is clearly in the image of π. By the remark following Proposition 2.5, there exists an $f' \in f + I$ such that $\mathrm{lt}(f') \notin \mathrm{Lt}(I)$. In particular $\mathrm{lt}(f') \notin (x_1^{m_1}, \ldots, x_n^{m_n})$, so in fact $\mathrm{lt}(f') \in K$.

Furthermore, since $f-f' \in I$ and $\mathrm{lt}(f') \notin \mathrm{Lt}(I)$, we have $\mathrm{lt}(f-f') \neq \mathrm{lt}(f')$. It follows that $\deg(f') \leqslant \deg(f)$ and so $\deg(f' - \mathrm{lt}(f')) < \deg(f)$. By induction on the degree of f, we may assume that $(f' - \mathrm{lt}(f')) + I$ is in the image of π, say $(f' - \mathrm{lt}(f')) + I = \pi(h)$ for some $h \in K$. Then $\pi(\mathrm{lt}(f') + h) = \pi(\mathrm{lt}(f')) + \pi(h) = (\mathrm{lt}(f') + I) + (f' - \mathrm{lt}(f') + I) = f' + I = f + I$, showing that $f + I$ is in the image of π. □

If G is a Gröbner basis for I, let $G_i = \{g \in G \mid \mathrm{lt}(g) = cx_i^m \text{ for some } c \in R, m \geqslant 0\}$ and let $L_i \subset R$ be the ideal generated by the leading coefficients of elements of G_i. Clearly $\mathrm{Lt}(G_i) = \mathrm{Lt}(G) \cap R[x_i]$ so $x_i \in \sqrt{\mathrm{Lt}(I)} = \sqrt{\mathrm{Lt}(G)}$ if and only if $x_i \in \sqrt{\mathrm{Lt}(G_i)}$. This can happen if and only if $L_i = (1)$, a condition we can verify. Thus we can decide whether $x_i \in \sqrt{\mathrm{Lt}(I)}$ just by examining a Gröbner basis for I. Furthermore it follows from that first part of the proof that if $x_i \notin \sqrt{\mathrm{Lt}(I)}$ then $x_i + I$ cannot be integral over R. Thus we have:

COROLLARY 5.3. *It is possible to decide whether $R[\mathrm{x}]/I$ is integral over R, and if not, to find an i such that $x_i + I$ is not integral over R.*

Applying the lemma, we get

COROLLARY 5.4. *If $I \cap R$ is zero-dimensional then it is possible to decide whether I is zero-dimensional, and if not, to find an i such that $I \cap R[x_i]$ is not zero-dimensional.*

When $I \cap R$ is primary then we can further simplify the criterion described above.

PROPOSITION 5.5. *Let $I \subset R[\mathrm{x}]$ be an ideal such that $I \cap R$ is zero-dimensional primary. Let G be a Gröbner basis for I. Then I is zero-dimensional if and only if for each I there exists a $g_i \in G$ such that $\mathrm{lt}(g_i) = c_i x_i^{m_i}$, $c_i \in R$ a unit modulo $I \cap R$.*

PROOF. Let G_i and L_i be as in the discussion preceding Corollary 5.3. Note that G_i contains $G \cap R$ and hence L_i contains $I \cap R$. Since $\sqrt{R \cap I}$ is maximal, $L_i = (1)$ if and only if $L_i \not\subset \sqrt{R \cap I}$, which can occur if and only if there is some $g_i \in G_i$ such that $\mathrm{lc}(g_i) \notin \sqrt{R \cap I}$. But this is equivalent to the requirement that $(\mathrm{lc}(g_i), R \cap I) = (1)$. □

Note that, with notation as above, every element of I whose leading term is divisible by $x_i^{m_i}$ is reducible modulo $\{g_i\} \cup (G \cap R)$. In particular, if G is a minimal Gröbner basis then all elements of G_i other than g_i have degree in x_i strictly smaller than m_i. Thus to decide whether I is zero-dimensional using a minimal Gröbner basis, one needs only to check that G_i contains exactly one element of the maximal degree, and that its leading coefficient together with $G \cap R$ generates the unit ideal—it is not necessary to check the leading coefficients of any other elements of G_i. Conversely, if I is known to be zero-dimensional then g_i can be uniquely identified as the highest degree element of G_i—there is no need to verify the condition on its leading coefficient.

We now investigate the structure of zero-dimensional primary ideals. When we say a polynomial has some property modulo an ideal J in R, we mean that its image as a polynomial in R/J has that property. We first note the following univariate results.

LEMMA 5.6. *Let $I \subset R[\mathrm{x}_1]$ be an ideal such that $I \cap R$ is zero-dimensional. Suppose $x_1^m \in \mathrm{Lt}(I)$, $x_1^{m-1} \notin \mathrm{Lt}(I)$. Then every $f \in I$ with $\deg(f) < m$ is a zero-divisor modulo $I \cap R$.*

PROOF. Let $L \subset R$ be the ideal generated by the leading coefficients of elements of I of degree less than m. We claim that if $f \in I$ has degree less than m then $f \equiv 0 \bmod L$. Let $f = c_1 x_1^{m-1} + \cdots + c_m$. Then c_1 is either 0 or it is the leading coefficient of f, so $c_1 \in L$. By assumption, there exists a $g \in I$ with $\mathrm{lt}(g) = x_1^m$. Let $f' = x_1 f - c_1 g$. Then $f' \in I$ and $f' = c_1' x_1^{m-1} + \cdots + c_m'$ with $c_i' \equiv c_{i+1} \bmod L$. It follows by induction that $c_i \in L$ for all i, proving the claim. Now if $L = (1)$ then I would contain a monic polynomial of degree less than m, contrary to assumption. Thus L is a proper ideal. Since $I \cap R \subset L$ with $I \cap R$ zero-dimensional, L is contained in some associated prime of $I \cap R$. Thus there exists an $a \notin I \cap R$ such that $aL \subset I \cap R$. Then $af \equiv 0 \bmod I \cap R$ whenever $\deg(f) < m$. □

LEMMA 5.7. *Let $I \subset R[x_1]$ be a zero-dimensional ideal such that $I \cap R$ is zero-dimensional primary. Let G be a minimal Gröbner basis for I and let $g_1 \in G$ be as in Proposition 5.5. Then $\sqrt{I} = \sqrt{(g_1, I \cap R)}$.*

PROOF. Let $\mathrm{lt}(g_1) = c_1 x_1^{m_1}$. By assumption, c_1 is a unit modulo $I \cap R$, so $x_1^{m_1} \in \mathrm{Lt}(g_1, I \cap R) \subset \mathrm{Lt}(I)$. $\mathrm{Lt}(I)$ cannot contain any smaller powers of x_1 since otherwise g_1 would be reducible, contradicting the minimality of G. Thus by Lemma 5.6, every $f \in I$ of degree less than m_1 is a zero-divisor modulo $I \cap R$. But since $I \cap R$ is primary, the set of zero-divisors modulo $I \cap R$ is exactly $\sqrt{I \cap R}$. Thus $f \in I$, $\deg(f) < m_1$ implies $f \equiv 0 \bmod \sqrt{I \cap R}$. Let $f \in I$. By Proposition 2.5, there exists $f' \equiv f \bmod (g_1, I \cap R)$ such that f' is reduced modulo $(g_1, I \cap R)$. Since $x_1^{m_1} \in \mathrm{Lt}(g_1, I \cap R)$, f' has degree less than m_1 so $f' \equiv 0 \bmod \sqrt{I \cap R}$. Thus $f \in (g_1, I \cap R) + \sqrt{I \cap R} = (g_1, \sqrt{I \cap R})$. In other words we have

$$I \subset (g_1, \sqrt{I \cap R}) \subset \sqrt{I}.$$

Taking radicals proves the lemma. □

We are now able to completely characterize zero-dimensional primary ideals in terms of verifiable conditions on their lexicographical Gröbner bases.

PROPOSITION 5.8. *Let $I \subset R[x]$ be a zero-dimensional ideal such that $I \cap R$ is zero-dimensional primary. Let G be a minimal Gröbner basis for I with respect to the lexicographical order with $x_1 > \cdots > x_n$, and let $g_1, \ldots, g_n \in G$ be as in Proposition 5.5. Then I is primary if and only if for all i, g_i is a power of an irreducible polynomial modulo $\sqrt{I \cap R[x_{i+1}, \ldots, x_n]}$. If this is the case then for every $h \in G \cap R[x_i, \ldots, x_n] - \{g_i\}$, $h \equiv 0 \bmod \sqrt{I \cap R[x_{i+1}, \ldots, x_n]}$.*

PROOF. Let $R' = R[x_2, \ldots, x_n]$, $I' = I \cap R'$. In view of Proposition 3.1, we may proceed by induction to conclude that the proposition holds for I' and $g_2, \ldots, g_n \in G \cap R'$. Thus we only need to show that I is primary if and only if I' is primary and g_1 is the power of an irreducible polynomial modulo $\sqrt{I'}$, in which case $h \equiv 0 \bmod \sqrt{I'}$ for $h \in G - \{g_1\}$.

Clearly if I is primary then so is I', so assume I' is primary. Let $\mathrm{lt}(g_1) = c_1 x_1^{m_1}$. If h is an element of G other than g_1, then it must have degree less than m_1 in x_1, since otherwise it would be reducible by (g_1, I'). Thus by Lemma 5.6 (and the assumption that I' is primary) $h \equiv 0 \bmod \sqrt{I'}$, proving the second part of the proposition. Since I is zero-dimensional, it is primary if and only if its radical is prime. By Lemma 5.7, $\sqrt{I} = \sqrt{(g_1, I')} = \sqrt{(g_1, \sqrt{I'})}$. Thus I is primary if and only if $(g_1, \sqrt{I'})$ is primary, or equivalently, if and only if the ideal generated by g_1 in $(R'/\sqrt{I'})[x_1]$ is primary. □

PROPOSITION 5.9. *Let $I \subset R[x]$ be a zero-dimensional ideal such that $I \cap R$ is zero-dimensional prime. Let G be a minimal Gröbner basis for I with respect to the lexicographical order with $x_1 > \cdots > x_n$, and let $g_1, \ldots, g_n \in G$ be as in Proposition 5.5. Then I is prime if and only if for all i, g_i is irreducible modulo $I \cap R[x_{i+1}, \ldots, x_n]$. If this is the case then $G = \{g_1, \ldots, g_n\} \cup (G \cap R)$.*

PROOF. Suppose I is prime. By Proposition 5.8, $g_i \equiv h_i^{k_i}$ for some h_i irreducible modulo $I \cap R[x_{i+1}, \ldots, x_n]$. Since I is prime, we must have $h_i \in I$. If $k_i > 1$ then g_i would be reducible by h_i, an element of smaller degree, contradicting the minimality of G. Thus $k_i = 1$ and so g_i is irreducible mod $I \cap R[x_{i+1}, \ldots, x_n]$.

Conversely, suppose $I \cap R[x_{i+1}, \ldots, x_n]$ is prime and g_i is irreducible modulo $I \cap R[x_{i+1}, \ldots, x_n]$. Then $(g_i, I \cap R[x_{i+1}, \ldots, x_n]) \subset R[x_i, \ldots, x_n]$ is prime. Furthermore, if h is an element of $G \cap R[x_i, \ldots, x_n]$ other than g_i, then by the previous proposition $h \equiv 0 \bmod I \cap R[x_{i+1}, \ldots, x_n]$. In particular h is reducible modulo $G \cap R[x_{i+1}, \ldots, x_n]$, so from the minimality of G it follows that $h \in G \cap R[x_{i+1}, \ldots, x_n]$. Thus $G \cap R[x_i, \ldots, x_n] = \{g_i\} \cup (G \cap R[x_{i+1}, \ldots, x_n])$ and consequently $I \cap R[x_i, \ldots, x_n] = (g_i, I \cap R[x_{i+1}, \ldots, x_n])$ is prime. The proposition now follows by induction. □

6. Zero-dimensional Primary Decomposition

In this section we assume that for any given maximal ideal $M \subset R$, it is possible to factor univariate polynomials over finitely generated algebraic extensions of R/M. This will be the case for instance if R is a finitely generated algebra over a prime field or $\mathbf{Z}$ (see Davenport & Trager, 1981).

We now present an algorithm for computing the irredundant primary decomposition of zero-dimensional ideals in $R[x]$. The algorithm works by computing the primary decomposition of $I \cap R[x_n]$, extending it to a (not necessarily primary) decomposition of all of I, and then proceeding by induction to construct a complete primary decomposition of each component. The following proposition describes the induction step.

PROPOSITION 6.1. *Let $I \subset R[x]$ be a zero-dimensional ideal such that $I \cap R$ is M-primary, where $M \subset R$ is a maximal ideal. Then one can construct zero-dimensional $I_1, \ldots, I_m \subset R[x]$ and distinct maximal ideals $M_1, \ldots, M_m \subset R[x_n]$ such that $I = \bigcap_i I_i$ and $I_i \cap R[x_n]$ is M_i-primary.*

PROOF. Let $I^c = I \cap R[x_n]$. By Lemma 5.7, we can find $g \in I^c$ such that $\sqrt{I^c} = \sqrt{(g, M)}$. Let $g(x_n) \equiv \prod p_i(x_n)^{s_i} \bmod M$ be the complete factorization of g modulo M, that is the images of $p_i(x_n)$ in $(R/M)[x_n]$ are pairwise comaximal irreducible non-units. Since $\prod p_i^{s_i} \in (g, M) \subset \sqrt{I^c}$, $(\prod p_i^{s_i})^s \in I^c$ for some s. Now since p_i, p_j are comaximal modulo M, and I contains a power of M, p_i, p_j are comaximal mod I. Thus $\bigcap_i (p_i^{s_i s}, I) = (\prod p_i^{s_i s}, I) = I$. Let $I_i = (p_i^{s_i s}, I)$, $M_i = (p_i, M)R[x_n]$. M_i is clearly maximal, and since $I_i \cap R[x_n]$ contains a power of M_i, it is either M_i-primary or the unit ideal. We have $\prod_{j \neq i} p_j^{s_j s} I_i \subset I$, so if $I_i = (1)$ then $\prod_{j \neq i} p_j \in \sqrt{I^c} = \sqrt{(g, M)}$. This contradicts the assumption that p_i is not a unit modulo M. Thus I_i is M_i-primary. □

By recursively applying the proposition to M_i, I_i over the base ring $R[x_n]$, we can compute the complete primary decomposition of I along with the associated primes.

ALGORITHM ZPD $(R; \mathrm{x}; M)$; *Zero-dimensional primary decomposition*

Input: Ring R; variables $\mathrm{x} = x_1, \ldots, x_n$; ideal $I \subset R[\mathrm{x}]$; ideal $M \subset R$
Assumptions: M is maximal, I is zero-dimensional, $I \cap R$ is M-primary.
Output: $\{(Q_1, M_1), \ldots, (Q_m, M_m)\}$, Q_i, M_i ideals in $R[\mathrm{x}]$ such that M_i is maximal, $M_i \neq M_j$, Q_i is M_i-primary, and $I = \bigcap_i Q_i$.

Step 1: *If* $n = 0$ then return $\{(I, M)\}$
Step 2: Compute a minimal Gröbner basis G for $I \cap R[x_n]$. [Proposition 3.1(ii)]
Step 3: Select the $g \in G$ of largest degree.
Step 4: Compute the complete factorization of g mod M, $g = \Pi p_i^{s_i}$ in $(R/M)[x_n]$, $p_i \in R[x_n]$.
Step 5: Find s such that $(\Pi p_i^{s_i})^s \in I \cap R[x_n]$.
Step 6: Let $I_i = (p_i^{s_i s}, I)$, $M_i = (p_i, M)R[x_n]$.
Step 7: Return $\bigcup_i$ ZPD $(R[x_n]; x_1, \ldots, x_{n-1}; I_i; M_i)$.

REMARK. The union in Step 7 is disjoint, that is, it is not necessary to check for and remove duplicates.

7. Zero-dimensional Ideals Over Fields of Characteristic 0

In this section we assume that K is a field of characteristic zero and that all Gröbner bases G are normalised so that $\mathrm{lc}(g) = 1$ for all $g \in G$.

If I is an ideal in $K[\mathrm{x}] = K[x_1, \ldots, x_n]$, let us denote $I_i = I \cap K[x_i, \ldots, x_n]$. If I is a zero-dimensional prime then by Proposition 5.9 every minimal lexicographical Gröbner basis for I has the form $\{g_1(x_1, \ldots, x_n), g_2(x_2, \ldots, x_n), \ldots, g_n(x_n)\}$, with g_i monic as a polynomial in x_i and irreducible modulo I_{i+1}. We can in fact obtain the following stronger result:

PROPOSITION 7.1 *Let I be a prime zero-dimensional ideal in $K[\mathrm{x}]$, $G = \{g_1(x_1, \ldots, x_n), \ldots, g_n(x_n)\}$ a minimal Gröbner basis for I with respect to the lexicographical order. Then "almost all" linear transformations of coordinates, $g_i = x_i - p_i(x_{i+1}, \ldots, x_n)$ for $i < n$.*

PROOF. By (the proof of) the primitive element theorem (Zariski & Samuel, 1975), for almost all $a_1, \ldots, a_n \in K$,

$$K[\mathrm{x}]/I \simeq K\left(\sum a_i x_i\right).$$

If we choose new coordinates $z_1, \ldots, z_n$ such that $z_n = \Sigma\, a_i x_i$, then we have:

$$K[z_1, \ldots, z_n]/I \simeq K(z_n).$$

Since $z_i \in K(z_n)$ for every i, we have that $z_i = f_i(z_n)$ holds in $K[z_1, \ldots, z_n]/I$ and hence I contains polynomials of the form $z_i - f_i(z_n)$ for all $i < n$. If G is a Gröbner basis relative to coordinates $z_1, \ldots, z_n$ then $z_i - f_i(z_n)$ is reducible mod G. Since the only element of G which could reduce z_i is g_i, we have $\mathrm{lt}(g_i) = z_i$ as required. □

We can now introduce the notion of "general position".

DEFINITION 7.2. If I is a prime zero-dimensional ideal in $K[\mathrm{x}]$ such that its lexicographical minimal Gröbner basis satisfies Proposition 7.1, we say that I is in general position.

We say that I, an arbitrary zero-dimensional ideal, is in general position if all of its associated primes are in general position and their contractions to $K[x_n]$ are pairwise comaximal.

COROLLARY 7.3. *If I is a primary zero-dimensional ideal in general position, then the g_i in Proposition 5.8 are powers of linear equations modulo $\sqrt{I_{i+1}}$ for $i < n$.*

As an example, consider the ideal $I = (x_1^2 + 1, x_2) \subset Q[x_1, x_2]$. x_2 is irreducible over Q and $x_1^2 + 1$ is irreducible over $Q[x_2]/(x_2)$, so by Proposition 5.9 I is a zero-dimensional prime ideal. It is not in general position since $x_1^2 + 1$ is not linear in x_1. If we make the substitution $x_2 = ax_1 + x_2$ and consider the ideal $I_a = (ax_1 + x_2, x_1^2 + 1)$, we find that $G_a = \{x_2^2 + a^2, ax_1 + x_2\}$ is the Gröbner basis for I_a whenever $a \neq 0$. In that case G_a is as required by Definition 7.2, so we see that any non-zero value of a is sufficient to bring I into general position.

REMARK. From the proof of Proposition 7.1 it follows that in order to put a zero-dimensional prime ideal in general position it is sufficient to replace x_n by $x_n + \Sigma\, c_i x_i$ for random $c_i \in K$. We remark also that it is always possible to put any zero-dimensional ideal in general position. The intent is to separate all the zeros in an algebraic closure by the last coordinate. To do so, one simply chooses c_i such that the values $x_n + \Sigma\, c_i x_i$ are distinct as $(x_1, \ldots, x_n)$ ranges over the set of zeros of the ideal in the algebraic closure of K. The set of "bad" choices form a proper algebraic subset of K^{n-1} and thus "almost all" choices of c_i are good.

PROPOSITION 7.4. *Let $I \subset K[x]$ be a zero-dimensional ideal in general position, G a lexicographical Gröbner basis for I, and let $g_1, \ldots, g_n \in G$ be in Proposition 5.5. If $g_n = \Pi\, p_i^{s_i}$ is the irreducible decomposition of g_n then $I = \bigcap_i (p_i^{s_i}, I)$ is the primary decomposition of I.*

PROOF. $(p_i^{s_i}, I)$ is a zero-dimensional ideal and by definition of general position it is contained in exactly one prime ideal. Thus it must be a primary ideal. □

If we are given a zero-dimensional ideal I, not necessarily in general position, then the above construction will yield a decomposition but not necessarily into primary components. If the minimal Gröbner basis for $(p_i^{s_i}, I)$ is not of the form predicted by Corollary 7.3, then I is not in general position. We can then proceed by choosing a different set of coordinates (or by reverting to the non-probabilistic algorithm ZPD). We remark however that a random substitution "almost always" works.

ALGORITHM ZPDF $(K; x; I)$. *Zero-dimensional primary decomposition over a field*

Input: Field K; variables $x = x_1, \ldots, x_n$; ideal $I \subset K[x]$
Assumptions: K is a field of characteristic zero, I is zero-dimensional.
Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset K[x]$ is a primary ideal, $I = \bigcap_i Q_i$ and $\sqrt{Q_i} \neq \sqrt{Q_j}$.
Step 1: Select random $c_1, \ldots, c_{n-1} \in K$ and replace x_n by $x_n + \Sigma\, c_i x_i$.
Step 2: Compute $I \cap K[x_n] = (g)$. [Proposition 3.1(ii)]
Step 3: Compute the complete factorization of g, $g = \Pi\, p_i^{s_i}$
Step 4: If $(p_i^{s_i}, I)$ is not a primary ideal in general position [Corollary 7.3] then go to Step 1.

Step 5: Replace x_n by $x_n - \Sigma\, c_i x_i$.
Step 6: Return $\{(p_i^{s_i}, I)\}$.

REMARK. In Step 4, it would be sufficient to test $(p_i^{s_i}, I)$ for being primary (using Proposition 5.8), but since the simpler test of Corollary 7.3 will be satisfied in almost all cases, it is preferable.

8. Primary Decomposition in Principal Ideal Domains

In this section we show how to reduce the general primary decomposition problem to the zero-dimensional case when the coefficient ring is a PID.

LEMMA 8.1. *Let S be a multiplicatively closed subset of R, $s \in S$. If $S^{-1}I \cap R \subset (I : s)$ then*

$$I = (I : s) \cap (I, s).$$

PROOF. $\subset$ is obvious. To prove $\supset$, suppose $f \in (I : s) \cap (I, s)$, so that $f = i + as$ with $i \in I$. Then $i + as \in (I : s) \Rightarrow is + as^2 \in I \Rightarrow as^2 \in I \Rightarrow a \in S^{-1}I \cap R \Rightarrow a \in (I : s) \Rightarrow as \in I \Rightarrow f \in I$. □

Combining the lemma with the construction of Proposition 3.7 we obtain the following fundamental decomposition mechanism.

PROPOSITION 8.2. *Let R be an integral domain, $(p) \subset R$ a principal prime ideal. For any given ideal $I \subset R[\mathrm{x}]$ it is possible to find $r \in R - (p)$ such that*

$$I = (I, r) \cap I^{ec}$$

where $I^{ec} = IR_{(p)}[\mathrm{x}] \cap R[\mathrm{x}]$.

PROOF. By Proposition 3.7 we can find $s \in R - (p)$ such that $I^{ec} = IR_s[\mathrm{x}] \cap R[\mathrm{x}]$. Thus we can compute I^{ec} by the method of Corollary 3.2(v). Since R is Noetherian, there exists an m such that $s^m I^{ec} \subset I$. Given a basis G for I^{ec}, we can compute m by testing whether $s^m G \subset I$ for successive values of m. By the lemma, $r = s^m$ is as required. □

PROPOSITION 8.3. *Let R be a PID, I an ideal in $R[\mathrm{x}]$, $(p) \subset R$ a maximal ideal. If $I \cap R$ is (p)-primary then it is possible to compute a primary decomposition for I.*

PROOF. If I is zero-dimensional then we can compute its decomposition using one of the algorithms of previous sections. Otherwise, by Proposition 5.5 we can find an i such that $I \cap R[x_i]$ is not zero-dimensional. Let $R' = R[x_i]$ and $\mathrm{x}' = x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, so that $R'[\mathrm{x}'] = R[\mathrm{x}]$ and $I \cap R'$ is not zero-dimensional. Applying Proposition 8.2, we can find $r' \in R' - (p)R'$ such that $I = (I, r') \cap I^{ec} = IR'_{(p)}[\mathrm{x}'] \cap R'[\mathrm{x}']$. Thus to decompose I it is sufficient to separately decompose (I, r') and I^{ec}.

Since $(I, r') \cap R'$ contains both the (p)-primary ideal $I \cap R$ and the element $r' \notin (p)R'$, either $(I, r') \cap R'$ is zero-dimensional or it is the unit ideal. In the former case, we can compute the primary decomposition of (I, r') by induction on the number of x_k such that the contraction of the ideal to $R[x_k]$ is not zero-dimensional. In the latter case $I = I^{ec}$ and so we only need to compute the decomposition I^{ec}.

In order to decompose I^{ec} we only need to decompose $I^e = IR'_{(p)}[\mathrm{x}']$ and then contract the decomposition back to $R'[\mathrm{x}']$ using Proposition 3.7. Note that $R'_{(p)}$ is again a PID,

and $(p)R'_{(p)}$ is a maximal ideal. We claim that $I^e \cap R'_{(p)}$ is $(p)R'_{(p)}$-primary. Since $I \cap R$ is (p)-primary, I(and hence $IR'_{(p)}$) contains a power of p. Thus it is sufficient to show that $IR'[x'] \cap R' \subset (p)R'$. Let P be a non-zero-dimensional associated prime of $I \cap R'$. Then $P \supset (p)R'$. But $(p)R'$ is one-dimensional, so $P = (p)R'$, which proves the claim. Thus $I^e \subset R'_{(p)}[x']$ satisfies the hypotheses of the proposition and so we may decompose it by induction on the number of variables. □

COROLLARY 8.4. *If K is a field then it is possible to compute the primary decomposition of any ideal in $K[x]$.*

PROOF. Take $p = 0$ in the proposition. □

We remark that in the field case, the ring $R'_{(p)} = R[x_i]_{(p)}$ appearing in the algorithm described above is simply the field $K(x_i)$. Thus if the initial problem is presented over a coefficient field then all computations, including all the recursive invocations of the decomposition algorithm, take place with a field as the coefficient ring.

PROPOSITION 8.5. *Let R be a PID, I an ideal in $R[x]$. Then it is possible to compute a primary decomposition for I.*

PROOF. If $I \cap R$ is not zero-dimensional (i.e. $I \cap R = (0)$ and R is not a field) then apply Proposition 8.2 to $(0) \subset R$ to find $r \neq 0$ such that $I = (I, r) \cap (IR_{(0)}[x] \cap R[x])$. Since $R_{(0)}$ is a field (the quotient field of R), $IR_{(0)}[x]$ can be decomposed using the field algorithm above, and the results contracted to $R[x]$ using Proposition 3.7. We are then left with (I, r), which contracts to a zero-dimensional ideal in R.

Thus we may assume that $I \cap R$ is zero-dimensional, say $I \cap R = (\Pi p_i^{m_i})$ where $(p_i)R$ is maximal. Then $(p_i^{m_i}, I) \cap R$ is (p_i)-primary, so $(p_i^{m_i}, I)$ can be decomposed using the algorithm of Proposition 8.3. Since $I = \bigcap_i (p_i^{m_i}, I)$ we get a decomposition for I. □

REMARK. The decomposition obtained above is not irredundant.

ALGORITHM PPD $(R; x; I)$: *Primary decomposition over a PID*

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$.
Assumptions: R is a PID.
Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset R[x]$ is primary and $I = \bigcap_i Q_i$.
Step 1: Find $r \neq 0$ such that $I = (I, r) \cap (IR_{(0)}[x] \cap R[x])$. [Proposition 8.2]
Step 2: Let $\{Q_1, \ldots, Q_k\} =$ PPD-0 $(R_{(0)}; x; IR_{(0)}[x]; 0)$.
Step 3: Let $Q_i^c = Q_i \cap R[x]$. [Proposition 3.7]
Step 4: Compute $(I, r) \cap R = (r')$.
Step 5: If r' is a unit, return $\{Q_1^c, \ldots, Q_m^c\}$.
Step 6: Factor $r' = \Pi p_i^{m_i}$, p_i irreducible.
Step 7: For each i let $\{Q_1^i, \ldots, Q_{k_i}^i\} =$ PPD-0 $(R; x; (I, p_i^{m_i}); p_i)$.
Step 8: Return $\{Q_1^c, \ldots, Q_k^c\} \cup \bigcup_i \{Q_1^i, \ldots, Q_{k_i}^i\}$.

ALGORITHM PPD-0 $(R; x; I; p)$: *Primary decomposition over a PID, primary contraction case*

Input: Ring R; variables $x = x_1, \ldots, x_n$; ideal $I \subset R[x]$; $p \in R$

Assumptions: R is a PID, $(p)R$ is maximal, $I \cap R$ is (p)-primary.
Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset R[\mathrm{x}]$ is primary and $I = \cap Q_i$.
Step 1: If I is zero-dimensional [Proposition 5.5] then return its decomposition using ZPD or ZPDF.
Step 2: Find i such that $I \cap R[x_i]$ is not zero-dimensional [still Proposition 5.5]
Step 3: Let $R' = R[x_i]$, $\mathrm{x}' = x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, $I^e = IR'_{(p)}[\mathrm{x}']$.
Step 4: Find $r' \in R' - (p)R'$ such that $I = (I, r') \cap (I^e \cap R'[\mathrm{x}'])$. [Proposition 8.2]
Step 5: Let $\{Q_1, \ldots, Q_m\} = \text{PPD-0}\ (R'_{(p)}; \mathrm{x}'; I^e; p)$.
Step 6: Let $Q_i^c = Q_i \cap R'[\mathrm{x}']$. [Proposition 3.7]
Step 7: If $(I, r') = (1)$ then return $\{Q_1^c, \ldots, Q_m^c\}$.
Step 8: Let $\{Q'_1, \ldots, Q'_k\} = \text{PPD-0}\ (R; \mathrm{x}; (I, r'); p)$.
Step 9: Return $\{Q_1^c, \ldots, Q_m^c, Q'_1, \ldots, Q'_k\}$.

9. Applications to Computing Radicals and Associated Primes

The algorithm of the preceding section depends on repeated applications of the following formula

$$I = (I, s) \cap (I : s) \qquad (*)$$

to reduce the dimension of I. s is chosen so that the dimension of (I, s) is strictly less than that of I, and $(I : s) = I^{ec}$ is the contraction of the extension of I to a polynomial ring of lower dimension.

This reduction strategy can be applied to other constructions provided they are well-behaved under the basic operations employed by the reduction process. As an example, we consider the computation of the radical and of ideal. We first observe that (*) implies that

$$\sqrt{I} = \sqrt{(I, s)} \cap \sqrt{I : s}.$$

But $\sqrt{(I : s)} = \sqrt{I^{ec}} = (\sqrt{I^e})^c$. Thus computing radicals commutes with our reduction strategy. At the point where algorithm PPD-0 is ready to call ZPD or ZPDF, we have reduced the problem to a zero-dimensional ideal whose contraction to the underlying PID R is (p)-primary. Since algorithm ZPD can also compute the associated primes in the situation, we can simply compute the radical as the intersection of the associated primes.

Using ZPD, however, makes radical computation no easier than primary decomposition. Since square-free factorization of polynomials over perfect fields reduces to greatest common divisor computations, which are in general easier than polynomial factorization, we could hope for an easier way to compute radicals of ideals. Once we have arrived at the situation where we have an ideal I such that $I \cap R$ is (p)-primary, we can adjoin p to I and assume $I \cap R$ is maximal. We can now reduce I modulo p, which brings us to the case of zero-dimensional ideals in a polynomial ring over a field. When this field is perfect, there is a much simpler radical construction based on Lemma 92 of Seidenberg (1974). Since I is zero-dimensional, it contains non-constant univariate polynomials $f_i(x_i)$ in each variable x_i. We define

$$g_i = f_i / gcd(f_i, f_i')$$

where f_i' is the derivative of f_i taken with respect to x_i. Since our coefficient field is perfect, g_i will have all distinct roots in any splitting field. Seidenberg shows that $\sqrt{I} = (I, g_1, \ldots, g_n)$. Note that the f_i can be found using a single Gröbner basis

computation along with the solution of linear equations, as observed by Buchberger (1985).

References

Ayoub, C. (1982). The decomposition theorem for ideals in polynomial rings over a domain. *J. Algebra*, **76**, 99–110.

Ayoub, C. (1983). On constructing bases for ideals in polynomial rings over the integers. *J. Number Theory*, **17**, 204–225.

Buchberger, B. (1965). *Ein algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D Thesis, Universitat Innsbruck.

Buchberger, B. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequationes Math.* **4**, 374–383.

Buchberger, B. (1976). A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bulletin*, **39**, 19–29.

Buchberger, B. (1979). A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In: *Symbolic and Algebraic Computation*, Lecture notes in computer science, Springer-Verlag, Heidelberg. Vol. 72, pp. 3–21.

Buchberger, B. (1985). Gröbner bases: An algorithmic method in polynomial ideal theory. In: (Bose, N. K., ed.) *Multidimensional Systems Theory*, D. Reidel Publishing Co., pp. 184–232.

Davenport, J., Trager, B. (1981). Factorization over finitely generated fields. *Proceedings of the 1981 Symposium on Symbolic and Algebraic Computation — Snowbird, Utah*, pp. 200–205.

Kaplansky, I. (1968). *Commutative Rings.* Queen Mary College Math Notices, London.

Lazard, D. (1985). Ideal bases and primary decomposition: case of two variables, *J. of Symb. Comp.* **1**, 261–270.

Richman, F. (1974). Constructive aspects of Noetherian rings. *Proc. Am. Math. Soc.* **44**, 436–441.

Seidenberg, A. (1974). Constructions in algebra. *Trans. Am. Math. Soc.* **197**, 273–313.

Seidenberg, A. (1978). Constructions in a polynomial ring over the ring of integers. *Am. J. Math.* **100**, 685–703.

Seidenberg, A. (1984). On the Lasker-Noether Decomposition Theorem. *Am. J. Math.* **106**, 611–638.

Spear, D. (1977). A constructive approach to commutative ring theory. *Proc. 1977 MACSYMA Users' Conference*, 369–376.

Trinks, W. (1978). Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory*, **10**, 475–488.

Zacharias, G. (1978). *Generalized Gröbner bases in Commutative Polynomial Rings.* Bachelor's Thesis, MIT.

Zariski, O., Samuel, P. (1975). *Commutative Algebra, Volume I.* Graduate Texts in Mathematics Volume 28, Springer-Verlag, Neidelberg.